

Universal Squash Model For Optical Communications Using Linear Optics And Threshold Detectors

Chi-Hang Fred Fung,^{1,*} H. F. Chau,^{1,†} and Hoi-Kwong Lo^{2,‡}

¹*Department of Physics and Center of Computational and Theoretical Physics,
University of Hong Kong, Pokfulam Road, Hong Kong*

²*Center for Quantum Information and Quantum Control,
Department of Physics and Department of Electrical & Computer Engineering,
University of Toronto, Toronto, Ontario, M5S 3G4, Canada*

(Dated: November 15, 2010)

The transmission of photons through open-air or an optical fiber is an important primitive in quantum information processing. Theoretical description of such a transmission process often considers only a single photon as the information carrier and thus fails to accurately describe experimental optical implementations where any number of photons may enter a detector. It is important to bridge this big gap between experimental implementations and the theoretical description. One powerful method that emerges from recent efforts to achieve this goal is to consider a squash model that conceptually converts multi-photon states to single-photon states, thereby justifying the equivalence between theory and experiments. However, up to now, only a limited number of protocols admit a squash model; furthermore, a no-go theorem has been proven which appears to rule out the existence of a universal squash model. Here, we observe that an apparently necessary condition demanded by all existing squash models to preserve measurement statistics is too stringent a requirement for many protocols. By chopping this requirement, we show that rather surprisingly, a universal squash model actually exists for a wide range of protocols including quantum key distribution protocols, quantum state tomography, the testing of Bell's inequalities, and entanglement verification, despite the standard no-go theorem.

PACS numbers: 03.67.Dd, 02.50.Tt, 03.65.Ta, 42.50.Ex

I. INTRODUCTION

Quantum mechanics opens up new ways to process information. Quantum information processing (QIP) allows tasks not possible in classical information processing, such as non-local correlations [1, 2], and unconditionally secure schemes for cryptography [3–5], randomness generation [6], and data hiding [7, 8]. One of the greatest triumphs of QIP to date is quantum key distribution (QKD) (a.k.a. quantum cryptography), which allows two distant users to share a secret (as a classical bit string) by sending quantum states over a quantum channel. Due to the ease of generation, transmission, and detection, photons are often used as information carrier in many quantum communication [9] tasks including QKD (see, e.g., [10–12]), teleportation (see, e.g., [13–16]), superdense coding (see, e.g., [17–19]), and quantum networks (see, e.g., [20, 21]).

In many quantum communication schemes (such as the most well-known QKD protocol – the Bennett-Brassard-1984 protocol [3] – and quantum state tomography [22]), the analyses often work on the assumption that the quantum channel presents single-photon signals to a receiver. These signals are subsequently measured with single-photon measurements. However, in practice, ex-

perimental equipment fall short in guaranteeing such a pure single-photon environment. This is because practical photon sources occasionally emit more than one photon, and the detection setup for implementing the qubit measurement is usually composed of threshold detectors (such as standard InGaAs or silicon avalanche photo-diodes). Threshold detectors only produce a click if the input signal contains one or more photons; thus, they are incapable of revealing the number of photons entering the detection setup. This immediately raises a key question: does this mean that all single-photon-based quantum communication schemes cannot run as expected from their original design and analyses? For example, it is unclear whether a single-photon-based QKD protocol can still provide unconditional security when multi-photon signals are received from the quantum channel. Also, in quantum state tomography, it is unclear whether we can ascribe a single-photon description to a state that we measure when such a state comes from a source that occasionally emits multi-photon signals.

The problem was initially motivated by QKD [23–25], but was realized to be important in other QIP tasks such as entanglement verification [25, 26]. This is because many QIP tasks also rely on qubits as the basis of analysis but they do not carry the immediate security concern of QKD that an intelligent eavesdropper may meticulously align her strategy with the practical detectors' behaviour. Our goal is to bridge the idealization of qubit-based quantum communications and the physical realization where multi-photon signals may be emitted from

* chffung@hkucc.hku.hk

† hfchau@hkusua.hku.hk

‡ hklo@comm.utoronto.ca

the source and/or received from the quantum channel. Indeed, the significance of this gap was demonstrated by Semenov and Vogel [27] who showed that the mismatch between the theoretical single-photon consideration and the actual experimental reality with multi-photon signals might produce a fake violation of Bell's inequality and even quantum physics [28].

While we address this QKD-motivated problem in the QKD context, our discussion applies equally to other contexts including quantum state tomography. Indeed, later in the paper, we will show that quantum state tomography technique can be also be applied to a detection setup with threshold detectors. Also, we note that there is a deep connection between the security of QKD and the testing of Bell's inequality which was first mentioned by Ekert [4] in 1991 and was subsequently demonstrated through the idea of “self-testing” for QKD [29, 30], device-independent QKD based on Bell's inequality [31, 32], and state tomography based on Bell's inequality [33].

QKD can be either prepare-and-measure or entanglement-based. In the former, one party Alice prepares a quantum state and sends it to another party Bob who immediately measures it upon reception, and in the latter, an entanglement source generates a pair of entangled quantum states to be distributed to the two parties. The multi-photon problem arises on the source side for prepare-and-measure QKD protocols because a phase-randomized weak coherent source is often used to simulate a single-photon source. Since the multiple photons in an emitted signal are modulated to carry the same information, extra copies of quantum information is available to Eve. The multi-photon problem on the receiver side arises from the use of threshold detectors in both type of QKD schemes.

Existing efforts in setting up actual QKD experiments involving threshold detectors and multiple-photon sources as well as in proving the unconditional security of QKD schemes using ideal apparatus [34–38] will not be wasted if one can slightly modify the post-processing procedure, the security proof, or the existing experimental setup using currently available technologies. Along this line of thought, the multi-photon problem at the source (for prepare-and-measure schemes) was solved by Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [23] with great performance enhancement from using decoy states [39–41] (see also Ref. [42]).

On the other hand, the threshold detection problem at the receiver (for both prepare-and-measure and entanglement-based schemes) can be solved by conceptually assuming a quantum operation before Bob that maps Eve's multi-photon states to single-photon states. GLLP called this a squash operation [23] (see Fig. 1). If an actual squashing device were concatenated to the multi-photon quantum channel, we would have an effective single-photon quantum channel emitting only single photons. Such a physical squashing device would immediately make the receiving side of the experimen-

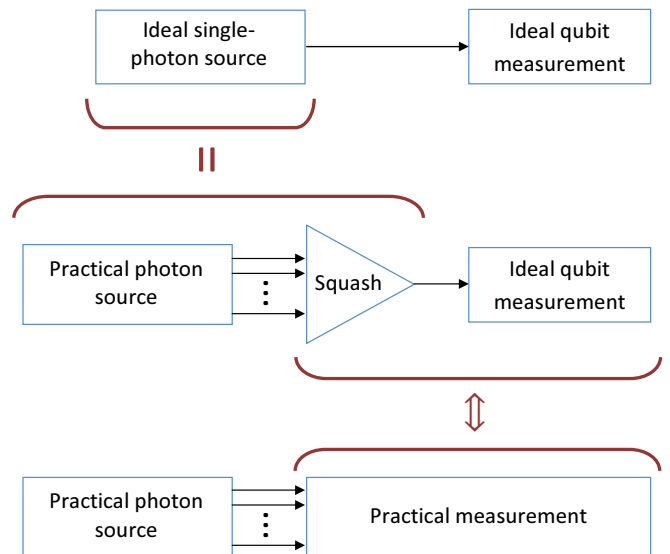


FIG. 1. The squash operation is a valid quantum operation that maps a multi-photon input state to a single-photon output state. The practical source together with the squash operation can be regarded as a single-photon source. The practical measurement on the multi-photon signal consists of threshold detectors and is argued in this paper to be statistically related to the combination of a universal squash operation and an ideal qubit measurement. Here, for simplicity, we use photon sources to also mean quantum channels.

tal setup compatible with the single-photon-based analyses. Although such a squashing device is impractical, the squashing approach can still be used to justify the conceptual presence of a squashing device, which is not always possible. Actually, the squash operation was fully justified only in a few security proofs for the BB84 [24, 25] and the BBM92 protocols [24]. These squash-operation-based security proofs are rather specific and do not provide a universal way to translate Eve's attack that outputs a multi-photon state to an attack that outputs a single-photon state. In particular, a squash map is proved to not exist for the six-state QKD scheme with active basis selection [25] which is a scheme first introduced by Bennett *et al.* [43] and later by Bruß [44]. In summary, previous works [45] show that a universal squash does not exist. This is a highly disappointing result because it appears to mean that for each protocol, one has to prove its security by a different method because one cannot apply a universal squash operation.

Despite the previous no-go theorem, here we show that a universal squash actually exists. The previous no-go theorem rests on a rather strong assumption that a squash map must be able to reproduce the precise measurement statistics (e.g., error rates). Preserving the statistics is a rather stringent requirement. The success of our approach lies in that we do not attempt to reproduce the exact statistics of the conceptual squash situation and we recognize that most quantum protocols do not need knowledge of exact statistics to func-

tion (bounds on statistics also suffice). Indeed, by relaxing this requirement and allowing a universal squash to produce only bounds on statistics, we show that, rather surprisingly, a universal squash actually exists. Consequently, many security proofs for single-photon QKD protocols (with active or passive basis selection) including the six-state protocol [44], three-states protocols [46], the SARG04 protocol (with four or six states) [47], the N -basis protocol [48], and protocols using decoy states [39–41], multi-partite quantum cryptographic protocols [49], reference-frame independent QKD [50], two-way protocols [51] directly carry over to practical implementations with a weak-coherent-state source and threshold detectors. This amounts to immense simplification. We emphasize that, in addition to QKD, our work also applies to quantum state tomography, the testing of Bell’s inequalities, and entanglement verification. Later in this paper, we will discuss the application of our universal squash model to quantum state tomography and the testing of Bell’s inequalities. Here, we remark that while the protocol-specific squashing approach of Ref. [25] has also been applied to entanglement verification [26], our approach has the advantage of being protocol independent (i.e., universal) and being applicable in many different contexts including quantum state tomography.

The organization of our paper is as follows. We discuss our proof on universal squash model in Sec. II followed by a discussion on the special treatment for the key bits in QKD in Sec. III. We then apply our universal squash model to QKD protocols in Sec. IV, quantum state tomography in Sec. V, and the testing of Bell’s inequality in Sec. VI. We conclude in Sec. VII.

II. UNIVERSAL SQUASH MODEL

We discuss our result assuming the following settings:

- The incoming photons are restricted to a single optical spatio-temporal mode and information is encoding in polarization. Note that there is no loss of generality in our discussion because phase encoding is mathematically equivalent to polarization encoding.
- For simplicity, we assume that Bob uses active basis selection for his measurements so that his detection system projects the incoming signal onto the eigenstates of only one basis. (We extend it to the case of passive basis selection in Appendix C.)
- Bob’s detection system consists of two threshold detectors plus possibly other linear optical elements (a representative structure is shown in Fig. 2). All photons in the same spatio-temporal mode entering each detector will be measured and collapsed individually. In other words, the projection operators describing the measurement of each individual photon commute and are independent of each

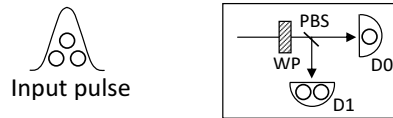


FIG. 2. Detection system used by Bob for one basis, where a set of waveplates (WP) select the basis and a polarizing beam-splitter (PBS) splits the signal into two arms for detection by two threshold detectors (D0 and D1). Here, the incoming signal consists of three photons and one is (two are) collapsed in detector D0 (D1).

other. Even though we focus on a two-detector receiver, for simplicity of discussion, our proof works with any number of detectors where multiple clicks may occur.

- The threshold detectors have perfect efficiencies and no dark counts. Therefore, all incoming photons are collapsed. Inefficient detectors may be modeled as perfectly efficient detectors followed by a beamsplitter, which may be absorbed into the channel.
- Quantum non-demolition (QND) measurements are implicitly assumed, without loss of generality, to be used by Bob to determine the input photon number throughout the proof. The presence of the QND measurements is consistent with the threshold detector model and does not affect the functioning of it.

Our proof can be illustrated pictorially as shown in Fig. 3. The essence is to link the real situation (with threshold detectors and the possibility of double-click events) to an ideal situation (consisting of a universal squash operation), which are Situation 3 and Situation 1, respectively, in Fig. 3. This linking is established by regarding the two situations as statistically equivalent to special cases of classical post-processing for a detection setup with photon-number-resolving (PNR) detectors (Situations 2 and 4). Both Situations 2 and 4 can be derived from Situation 5, which is a detection setup with PNR detectors that outputs the full information on the number of photons detected in each detector. We discuss the elements of our proof as follows.

A. State representation

We write an n -photon pure state in tensor product form and then impose bosonic symmetry by symmetrizing the state [52]. Similarly, an n -photon mixed state can be dealt with as a mixture of pure states. Let ρ denote the density matrix of an n -photon state. A squash operation is a quantum operation that takes an n -photon state as input and produces a single-photon state as output.

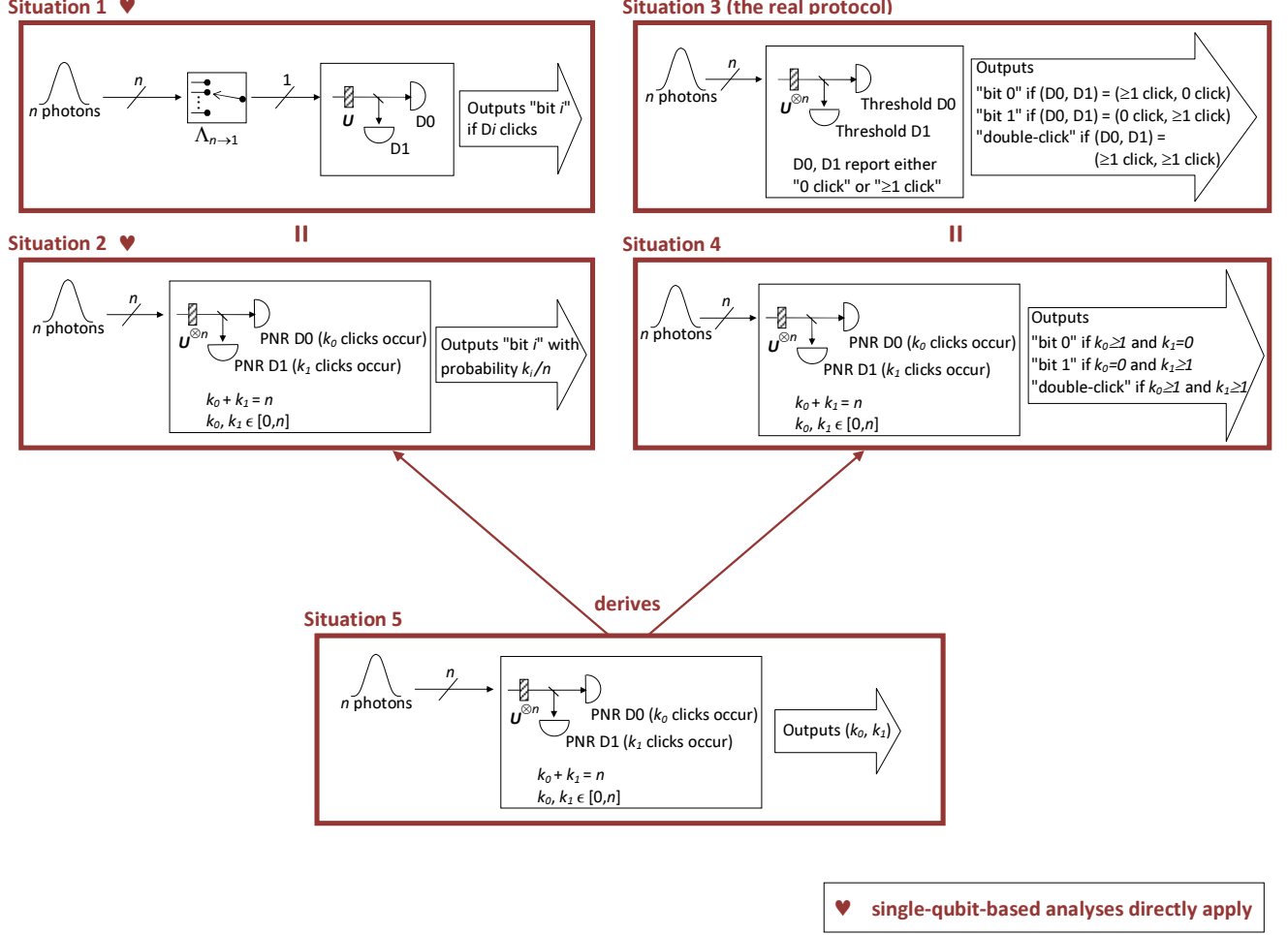


FIG. 3. Relationship map for the five situations used to prove our universal squash model. The goal is to link the real situation (Situation 3) with the ideal situation (Situation 1) consisting of the universal squash operation.

In Situation 1 (a virtual protocol), an n -photon state enters a detection system comprising the squash operation $\Lambda_{n \rightarrow 1}$, a set of waveplates (acting as unitary transform U), a polarizing beamsplitter, and two detectors. The universal squash operation $\Lambda_{n \rightarrow 1}$ maps n photons to one. We do not specify whether the detectors are photon-number-resolving (PNR) or threshold detectors since after the squash operation, only one photon remains. The output of the detection system is a bit value corresponding to the detector that has a click. This is a single-qubit situation since we can regard the squash operation as part of the channel. In Situation 2 (a virtual protocol), an n -photon state enters a detection system comprising a set of waveplates (acting as unitary transform $U^{\otimes n}$), a polarizing beamsplitter, and two PNR detectors, followed by a classical post-processor. The classical post-processor serves as the classical analog of the squash operation $\Lambda_{n \rightarrow 1}$ and outputs a bit value according to probabilities given by the detectors' clicks. More concretely, suppose that detectors D_0 and D_1 register k_0 and k_1 photons respectively. Then, the classical post-processor in Situation 2 outputs event "bit i " ($i = 0, 1$) with probability $k_i/(k_0 + k_1)$.

We show in Theorem 1 that the bit value outputs of Situations 1 and 2 have the same statistics for any n -photon input state and any unitary transform U (see Supplementary Materials for proof).

Situation 3 (the real protocol) is similar to Situation 2 with the PNR detectors replaced by threshold detectors. Situation 3 outputs event "bit i " if only detector D_i clicks ($i = 0, 1$) and event "double-click" if both detectors click. Situation 4 is also similar to Situation 2 with a difference in the post-processing part. Here, the post-processing only announces one of three events corresponding to a single-click for "0", a single-click for "1", and a double-click. It is easy to see that the Situations 3 and 4 produce the same output statistics for the same input state. In this paper, we consider only those protocols for which Situations 3 and 4 are equivalent.

Situation 5 is the mother protocol that derives Situations 2 and 4. Note that the detection parts of Situations 2, 4, and 5 are all the same; only their classical processing parts are different. In fact, the classical processing parts of Situations 2 and 4 can be generated by that of Situation 5 which outputs the full information on the numbers of detection clicks.

B. Universal squash operation

We define our *universal squash operation* as the mapping from ρ to ρ_{qubit} where $\rho_{\text{qubit}} = \text{Tr}(\rho)$ over any $n - 1$ photons is the reduced density matrix of one photon. It does not matter which $n - 1$ photons we trace over and the same ρ_{qubit} will result due to the bosonic symmetry. We denote this mapping as $\Lambda_{n \rightarrow 1}(\rho) = \rho_{\text{qubit}}$. Note that $\Lambda_{n \rightarrow 1}$ is a valid quantum operation.

C. Equivalence of Situations 1 and 2

Theorem 1. Situations 1 and 2 are equivalent and produce the same output statistics for any unitary transform and any n -qubit input state.

This result is non-trivial and its proof is discussed in Appendices A 1 and A 2. The main point is that a universal squash operation (Situation 1) can be regarded as a special classical post-processing method for a detection system with PNR detectors (Situation 2). Theorem 1 justifies an effective single-qubit channel since the squash operation in Situation 1 can be regarded as part of the channel. This means that it is valid to apply the result of any single-qubit-based analysis to Situation 2.

D. Equivalence of Situations 3 and 4

It is easy to see that the real situation with threshold detectors (Situation 3) is equivalent to another special classical post-processing method for a detection system with PNR detectors (Situation 4).

E. Relationship between Situations 2 and 4

Situations 2 and 4 are related through Situation 5 (shown in Fig. 3). Since both Situations 2 and 4 are special cases of classical post-processing for a detection system with PNR detectors, they can both be derived from the same situation – Situation 5. Thus, the statistics of Situation 4 can be used to infer some statistics about Situation 2. For QKD protocols, the statistics of interest is the error rate e_b between Alice and Bob in basis b . Thus, we aim at providing bounds on the error rates. A single-click in Situation 4 immediately tells us that a definite bit value would have been obtained in Situation 2 and this bit value is directly used for the evaluation of the error rates. On the other hand, a double-click in Situation 4 does not tell us which bit value it corresponds to in Situation 2, and there is no definite bit value to be used for the error-rate evaluation. To overcome this, we recognize that we do not need to know the definite bit value since all we care are bounds on the error rates. Our key idea is to bound the range of possible error rates by using the most pessimistic and optimistic values for double-click events.

Specifically, a double-click event contributes as an error bit for the calculation of the upper bound on the error rate and contributes as a correct bit for the lower bound. Suppose that the number of test bits for basis b is N_b , where $N_b = N_b^{s,c} + N_b^{s,e} + N_b^d$. Here, $N_b^{s,c}$, $N_b^{s,e}$, and N_b^d are the correct single-click events, erroneous single-click events, and double-click events, respectively. Then, the error rate of the test bits is bounded by

$$e_b^L = \frac{N_b^{s,e}}{N_b} \leq e_b \leq \frac{N_b^{s,e} + N_b^d}{N_b} = e_b^U. \quad (1)$$

Corollary 1. (Single-qubit description) We regard the original quantum channel followed by the squash operation $\Lambda_{n \rightarrow 1}$ in Situation 1 as the *effective single-qubit quantum channel*. Thus, we can ascribe a single-qubit description to the actual received signals and the associated channel error statistics are bounded by Eq. (1).

This allows us to apply any single-qubit-based security analysis to qubit-based QKD protocols whose qubit assumption is violated in practical implementation due to the reception of multi-photons.

Note that there are two such effective single-qubit quantum channels for entanglement-based QKD protocols (in which an entanglement source sends two signals one to Bob and one to Alice).

III. POST-SELECTION OF KEY BITS IN QKD

In QKD protocols, one subset of the data obtained from the quantum channel (called the test bits) is devoted to estimating the statistics of the channel and another subset (called the key bits) for key generation. The key bits are eventually transformed into the final secret key through a series of classical operations and communications.

The bounds established above given in Eq. (1) apply to the channel output states irrespective of whether they are used as test bits or key bits. Since we actually need to use the bit values of the key bits, we propose to discard all the double-click key bits for which we do not know the values. This post-selection procedure requires us to extend the bounds of Eq. (1) when applied to the remaining key bits since we need to take into account the most pessimistic and optimistic error statistics of the discarded bits.

More specifically, if we had known the value of every key bit in Situation 2, we would have directly applied a qubit-based security proof to distill a final secret key. However, we are in Situation 4 (or Situation 3, the real situation), and we do not know the key bit value for double-click events. To solve this problem, our strategy is to discard all double-click key bits and augment the error rate bounds of Eq. (1) for describing the remaining key bits. Eventually, we will come up with new bounds for the error rates for the key after discarding:

$$e_b^{\text{key,L}} \leq e_b^{\text{key}} \leq e_b^{\text{key,U}}. \quad (2)$$

To aid discussion, we designate one basis as the key-generating basis, denoted as basis b^* . All key bits are detected in this basis and thus all single- or double-click events are classified according to this basis. We first consider the b -basis error rate, where $b \neq b^*$. Because the key bits discarded according to whether it is a double-click event in the b^* -basis may have any error rate in other bases, the lower and upper bounds on the error rate e_b^{key} in the b -basis for the remaining key bits are:

$$\begin{aligned} e_b^{\text{key,L}} &= \frac{e_b^{\text{L}} N_{b^*}^{\text{key}} - N_{b^*}^{\text{key,d}}}{N_{b^*}^{\text{key,s}}} \\ e_b^{\text{key,U}} &= \frac{e_b^{\text{U}} N_{b^*}^{\text{key}}}{N_{b^*}^{\text{key,s}}}, \text{ for } b \neq b^* \end{aligned} \quad (3)$$

where $N_{b^*}^{\text{key,s}}$ ($N_{b^*}^{\text{key,d}}$) is the number of single-click (double-click) events among all the $N_{b^*}^{\text{key}} = N_{b^*}^{\text{key,s}} + N_{b^*}^{\text{key,d}}$ key bits measured in basis b^* . Here, the lower (upper) bound comes from assuming that the b^* -basis double-click events discarded correspond to erroneous (correct) bits in the b -basis.

The b^* -basis error rate of the key bits after discarding double clicks can be inferred from the b^* -basis error rate of the single-click test bits. In the asymptotic case, these two error rates are the same, and are given by excluding the double-click events in Eq. (1):

$$e_{b^*}^{\text{key}} = \frac{N_{b^*}^{\text{s,e}}}{N_{b^*}^{\text{s,c}} + N_{b^*}^{\text{s,e}}}. \quad (4)$$

Eqs. (2)-(4) describe the key bits measured in the b^* -basis after discarding double-click events. Classical post-processing steps derived from a qubit-based security proof can then be used to distill a final secret from the key bits according to these equations. Also, we only need to consider physical states that satisfy the error rate constraints given in Eqs. (2)-(4); unphysical states need not be considered.

The key distillation steps are usually composed of two parts: error correction (EC) and privacy amplification (PA). EC and PA are classical procedures for correcting errors between Alice's and Bob's initial keys and for removing Eve's information about their keys, respectively. The codes/schemes and the associated parameters for EC and PA are determined from Eqs. (2)-(4) according to the security proof for the particular QKD protocol.

A. QKD post-processing with error-rate ranges

We emphasize that our method involves EC and PA that operate on error rates given in ranges where the lower bound is not necessarily zero. Note that most realistic EC codes are already designed to correct errors up to a certain error rate starting from zero. Also, PA schemes based on phase error correction using random hashing or random codes [34–36] and those based on information-theoretic proofs using universal hashing [37, 38] chosen

according to the worst-case error rates automatically tolerate intermediate error rates.

Note that correlation between the different bases, which are reflected in the error rates and the structure of their respective bases (e.g., as in the six-state protocol), can be exploited by choosing the EC code and the PA scheme appropriately. To compute the asymptotic key generation rate, it is sufficient to consider the worst-case physical state (see examples in Sec. IV).

IV. QKD EXAMPLES

A. Six-state QKD protocol

Considering the asymptotic case, suppose that Alice and Bob observe that their measurement results on the test bits for bases X , Y , and Z all have the same erroneous single-click rate ϵ , double-click rate δ , and correct single-click rate $1 - \delta - \epsilon$. [53] This induces the following bounds on the asymptotic error probabilities on the key bits (before discarding double-clicks) according to Eq. (1):

$$\epsilon \leq e_X, e_Y, e_Z \leq \epsilon + \delta. \quad (5)$$

The key bits are measured in the Z -basis and double-click key bits are discarded. After discarding, the error rate in the Z -basis of the post-selected key bits is given by Eq. (4) due to direct inference from the test bits and the error rates in the other bases are bounded with Eq. (3):

$$\begin{aligned} e_Z^{\text{key}} &= \frac{\epsilon}{1 - \delta} \\ \frac{\epsilon - \delta}{1 - \delta} &\leq e_X^{\text{key}}, e_Y^{\text{key}} \leq \frac{\epsilon + \delta}{1 - \delta}. \end{aligned} \quad (6)$$

The key generation rate for the six-state protocol with one-way error reconciliation is (cf. Ref. [54]):

$$R_{\text{six-state}} = \min_{b_1, b_2, b_3} (1 - \delta) \left[1 - h \left(b_1, b_2, b_3, 1 - \sum_{i=1}^3 b_i \right) \right] \quad (7)$$

subject to $e_Z^{\text{key}} = b_1 + b_2$, $e_X^{\text{key}} = b_2 + b_3$, $e_Y^{\text{key}} = b_1 + b_3$, and Eq. (6), where $h(b_1, b_2, \dots) = -\sum_i b_i \log b_i$. The minimum is achieved with, under some condition, (see Appendix B)

$$b_1 = \frac{\epsilon}{1 - \delta} - b_2 \quad (8)$$

$$b_3 = \frac{\epsilon + \delta}{1 - \delta} - b_2 \quad (9)$$

$$b_2 = \frac{\epsilon - 2\delta}{2(1 - \delta)}. \quad (10)$$

Note that in the limit that δ goes to zero, $b_1 = b_2 = b_3$, and we recover the standard result in single-photon-based six-state QKD. This shows that at small double-click rates, the six-state protocol still gives a higher key

rate than the BB84 protocol [55]. In practice, the double-click rate with a weak-coherent-state source is usually pretty small, since the average source intensity is usually less than one photon per pulse and the fiber medium incurs signal loss. Thus, applying our universal squash model to the six-state protocol in practice does not incur much loss due to the pessimistic error-rate estimation and the discarding of double-click key bits. This shows the power of our universal squash model in security proofs.

B. The BB84 protocol

Similar to the example on the six-state protocol, suppose that Alice and Bob observe that their measurement results on the test bits for bases X , Y , and Z all have the same erroneous single-click rate ϵ , double-click rate δ , and correct single-click rate $1 - \delta - \epsilon$. This induces the following bounds on the asymptotic error probabilities:

$$\epsilon \leq e_X, e_Z \leq \epsilon + \delta. \quad (11)$$

The key bits are measured in the Z -basis and double-click key bits are discarded. After discarding, the error rate in the Z -basis of the post-selected key bits is ϵ due to direct inference from the test bits (cf. Eq. (4)) and the error rate in the X -basis is bounded with Eq. (3):

$$\begin{aligned} e_Z^{\text{key}} &= \frac{\epsilon}{1 - \delta} \\ \frac{\epsilon - \delta}{1 - \delta} &\leq e_X^{\text{key}} \leq \frac{\epsilon + \delta}{1 - \delta} \end{aligned} \quad (12)$$

The key generation rate with one-way reconciliation is thus [35, 36, 38, 56]

$$R_{\text{BB84}} = (1 - \delta) \left[1 - h_2 \left(\frac{\epsilon}{1 - \delta} \right) - h_2 \left(\frac{\epsilon + \delta}{1 - \delta} \right) \right]. \quad (13)$$

The squash model of Ref. [24, 25] for the BB84 protocol preserve the measurement statistics when the double-click events are randomly assigned a bit value. Their key rate without discarding double-click events is

$$R'_{\text{BB84}} = 1 - 2h_2(\epsilon + \delta/2). \quad (14)$$

Figure 4 shows that our universal squash model given in Eq. (13) has similar performance as or even sometimes outperforms the statistics-preserving squash model of Ref. [24, 25] given in Eq. (14). This is because we allow double-click key bits to be discarded in our model. For fair comparison, we also consider the key rate of the statistics-preserving squash model with discarding double-click key bits:

$$R''_{\text{BB84}} = (1 - \delta) \left[1 - h_2 \left(\frac{\epsilon}{1 - \delta} \right) - h_2 \left(\frac{\epsilon + \frac{\delta}{2}}{1 - \delta} \right) \right]. \quad (15)$$

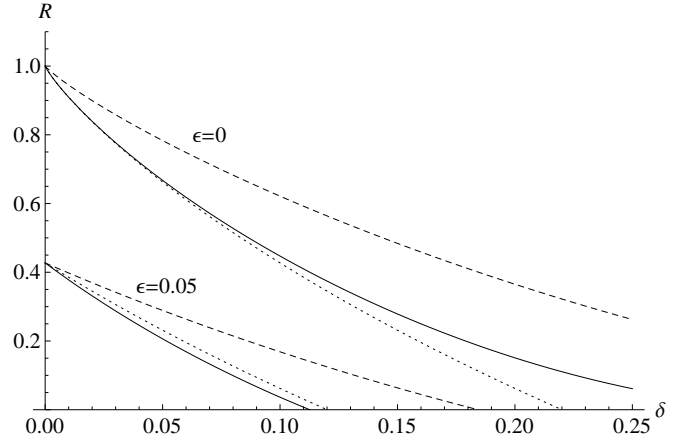


FIG. 4. Dependence of the key rate R per detected signal on the double-click rate δ . The solid curves are for our universal squash model (Eq. (13)) and the dotted curves and the dashed curves are for the BB84-specific squash model [24, 25] (Eq. (14) and Eq. (15) respectively).

Here, the first entropic term corresponds to bit error correction and the bit error rate is obtained with Eq. (4); the second entropic term corresponds to phase error correction and the phase error rate is upper bounded by assuming that all the double-click key bits discarded have no phase error and re-normalizing the phase error rate of the initial set of key bits $\epsilon + \frac{\delta}{2}$ by the size of the final set. Figure 4 compares the two models, and it shows that substantive difference exists between R_{BB84} and R''_{BB84} when the double-click rate is large. However, in practice, the double-click rate is usually quite small.

C. BB84 in realistic setting

We consider the performance of our universal squash model in the realistic setting with a weak coherent state source and the decoy-state method. Suppose that Alice uses a phase-randomized weak-coherent-state source that emits signals of photon number n with the Poisson distributed probability $p_{\mu,n} = \frac{e^{-\mu} \mu^n}{n!}$ where μ is the mean photon number. Typically, μ is small and on the order of 1 (e.g., $\mu = 0.5$). The yield, Y_n , is the probability that Bob gets a detection (either a single-click event or a double-click event) given that Alice sent an n -photon signal. For a state generated by the source with intensity μ , the gain, defined as the probability that Bob has a detection and Alice sent an n -photon state, is

$$Q_{\mu,n} = p_{\mu,n} Y_n. \quad (16)$$

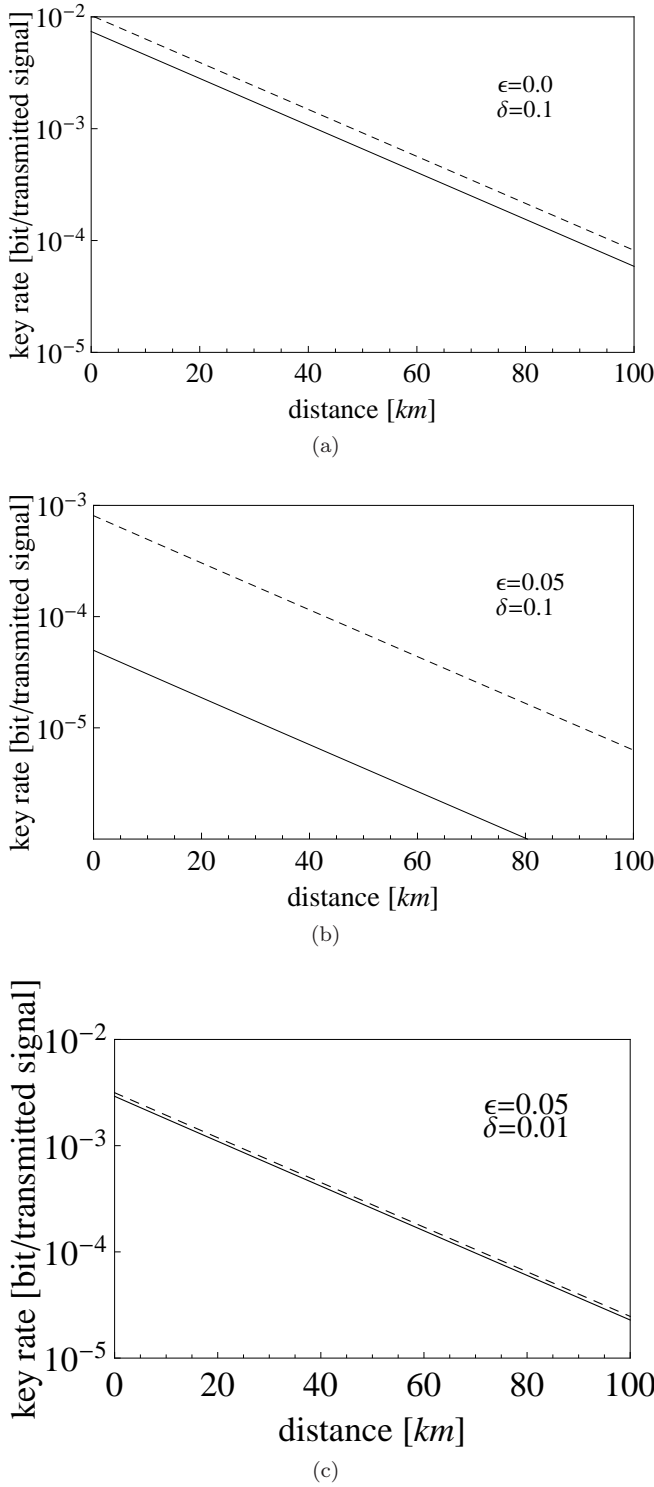


FIG. 5. Dependence of the key rate per transmitted signal on distance. The solid curves are for our universal squash model (Eqs. (23) and (25)) and the dashed curves are for the BB84-specific squash model [24, 25] (Eqs. (27) and (25)). Optimal μ is used at every distance. Here, we used the experimental parameters for signals at wavelength 1550 nm from the Gobby-Yuan-Shields experiments [57]: $\alpha = 0.21$ dB/km and $\eta_{\text{Bob}} = 4.5\%$.

The overall gain, single-click error rate, single-click correct rate, and double-click rate, are, respectively

$$Q_\mu = \sum_{n=0}^{\infty} p_{\mu,n} Y_n \quad (17)$$

$$Q_\mu F_\mu^{\text{s,e}} = \sum_{n=0}^{\infty} p_{\mu,n} Y_n F_n^{\text{s,e}} \quad (18)$$

$$Q_\mu F_\mu^{\text{s,c}} = \sum_{n=0}^{\infty} p_{\mu,n} Y_n F_n^{\text{s,c}} \quad (19)$$

$$Q_\mu F_\mu^{\text{d}} = \sum_{n=0}^{\infty} p_{\mu,n} Y_n F_n^{\text{d}} \quad (20)$$

where

$$F_n^{\text{s,e}} + F_n^{\text{s,c}} + F_n^{\text{d}} = 1 \quad \forall n \quad (21)$$

and the three terms in the last equation are the single-click error rate, single-click correct rate, and double-click rate on n -photon states sent by Alice.

To estimate the channel parameters, we use the infinite decoy state protocol [40] in which we vary the source intensity μ continuously to generate infinitely many decoy states that form a system of linear equations from Eqs. (17)-(20). We expect that a finite decoy state method will give similar results [41, 58]. The decoy states are solely for parameter estimation, and solving this system of equations gives Y_n , $F_n^{\text{s,e}}$, $F_n^{\text{s,c}}$, and F_n^{d} for all n . Since we now know the single-click error rate, single-click correct rate, and double-click rate for the single-photon states emitted by Alice, we can compute the worst-case single-photon error rates in our universal squash model in the same manner as in the previous analysis for single-photon sources. According to Eq. (1), they are bounded by

$$F_1^{\text{s,e}} \leq e_{X,1}, e_{Z,1} \leq F_1^{\text{s,e}} + F_1^{\text{d}}. \quad (22)$$

The key bits are measured in the Z -basis and double-click key bits are discarded. After discarding, the single-photon error rate in the X -basis is bounded as in Eq. (3) to be

$$e_{X,1}^{\text{key}} \leq \frac{F_1^{\text{s,e}} + F_1^{\text{d}}}{1 - F_1^{\text{d}}} = e_{X,1}^{\text{key,U}}. \quad (23)$$

Since we correct all Z -basis errors for all states with any photon number, the overall error rate in the Z -basis of the post-selected key bits is given by Eq. (4) to be

$$e_{Z,\bar{\mu}}^{\text{key}} = \frac{F_{\bar{\mu}}^{\text{s,e}}}{F_{\bar{\mu}}^{\text{s,e}} + F_{\bar{\mu}}^{\text{s,c}}}. \quad (24)$$

Here, we use $\bar{\mu}$ to represent the intensity for the key-generating signal states. The key rate, according to Gottesman-Lo-Lütkenhaus-Preiskill [23], is

$$R_{\text{BB84,decoy}} = -Q_{\bar{\mu}}(1 - F_{\bar{\mu}}^{\text{d}})h_2\left(e_{Z,\bar{\mu}}^{\text{key}}\right) + Q_{\bar{\mu},1}(1 - F_1^{\text{d}})\left[1 - h_2\left(e_{X,1}^{\text{key,U}}\right)\right]. \quad (25)$$

We assume the following simulation model to represent Eve's control over the channel parameters, Y_n , $F_n^{s,e}$, $F_n^{s,c}$, and F_n^d . Each photon has a certain transmission probability $\eta_{\text{ch}} = 10^{-\frac{\alpha l}{10}}$ of not being lost in the fiber optic channel where α in dB/km is the loss coefficient of the fiber and l in km is the length of the fiber. Also, Bob's detectors have a certain detection efficiency η_{Bob} for detecting an input photon. Thus, the probability for a single photon to be detected by Bob is $\eta = \eta_{\text{ch}}\eta_{\text{Bob}}$. The yield is

$$Y_n = 1 - (1 - \eta)^n. \quad (26)$$

Since we do not assume the detectors to have dark counts, a single-photon signal emitted by Alice will at most produce one click on Bob's side if the signal goes through a passive channel. Thus, for illustration purpose, we assume that Eve actively introduces multiple photons to Bob and her attack induces $F_n^{s,e} = \epsilon$, $F_n^d = \delta$, and $F_n^{s,c} = 1 - \epsilon - \delta$ for all n . Figure 5 shows the key generation rates using this simulation model. Results for our universal squash model and the statistics-preserving squash model of Ref. [24, 25] specific to BB84 are shown. The key rate for the latter case is given by Eq. (25) with

$$e_{X,1}^{\text{key,U}} = \frac{F_1^{s,e} + F_1^d/2}{1 - F_1^d}. \quad (27)$$

As shown in the figure, the performance degradation of our universal squash model is small when the single-click error rate ϵ is small or the double-click rate δ is small. Note that there is no cutoff distance for both cases since we do not assume the detectors to have dark counts.

V. QUBIT STATE TOMOGRAPHY

In many qubit state tomography experiments (e.g., [59, 60]), photons often are not generated from true single-photon sources. When non-ideal sources and threshold detectors are used, without a squash model it is unclear whether one can talk about determining the qubit state since multi-photon signals may be emitted. On the other hand, our universal squash approach allows quantum state tomography techniques to be rigorously applied even to detection setups with non-ideal sources and threshold detectors. After a squash operation, a state is reduced to that of a qubit and one can determine tomographically the state of the resulting qubit. We emphasized that our universal squash model can also be applied to multi-qubit tomography [61]. The overall argument for applying our universal squash model to tomography is similar to that for QKD, with a difference in the statistics of interest involved. Here, as shown below, we are interested in the average measurement value instead of the error rate. Standard qubit state tomography using the Stokes parameters [62] involves measuring the polarization of identical single-photon states ρ in an ensemble using the three bases X , Y , and Z .

The Pauli matrices are $W = |0_W\rangle\langle 0_W| - |1_W\rangle\langle 1_W|$ where $W = X, Y, Z$, and $|b_X\rangle = (|0_Z\rangle + (-1)^b|1_Z\rangle)/\sqrt{2}$, $|b_Y\rangle = (|0_Z\rangle + (-1)^b i|1_Z\rangle)/\sqrt{2}$, $b = 0, 1$. The density matrix of the qubit ρ can be tomographically determined to be

$$\rho = \frac{1}{2}I + \frac{1}{2} \sum_{W=X,Y,Z} \text{Tr}(\rho W)W. \quad (28)$$

We now discuss how to bound the parameters $\text{Tr}(\rho W)$ when non-ideal sources and threshold detectors are used. Suppose that we measure basis W with a threshold detection setup in Fig. 2 for N_W number of signals. According to the measurement outcomes, we decompose the signals into three parts: $N_W = N_W^{s,+} + N_W^{s,-} + N_W^d$ where $N_W^{s,\pm}$ and N_W^d are the single-click events corresponding to the ± 1 outcome of the measurement W and double-click events, respectively. Then, $\text{Tr}(\rho W)$ is bounded by

$$\begin{aligned} \frac{N_W^{s,+} - N_W^{s,-} - N_W^d}{N_W} &\leq \text{Tr}(\rho W) \\ &\leq \frac{N_W^{s,+} - N_W^{s,-} + N_W^d}{N_W}. \end{aligned} \quad (29)$$

Using these bounds and $\text{Tr}(\rho I) = 1$, we can obtain a set of consistent qubit states using Eq. (28). Essentially, our universal squash model allows one to ascribe a qubit description to the output states.

VI. TESTING OF BELL'S INEQUALITY

We can use our result to derive bounds on Bell's inequality [1] violation which may subsequently be used for qubit state tomography. Here, the statistics of interest comes from the Clauser-Horne-Shimony-Holt (CHSH) inequality [2] (perhaps the most famous Bell-type inequality [1]) which considers the statistics $\chi = E[A_1 B_1] + E[A_1 B_2] + E[A_2 B_1] - E[A_2 B_2]$, where $E[A_i B_j] = \langle \psi | A_i \otimes B_j | \psi \rangle$ is the expectation value of the bipartite state $|\psi\rangle$ with $\{-1, +1\}$ -valued observables A_i, B_j , $i, j = 1, 2$. The maximum value of χ in quantum mechanics is $2\sqrt{2}$ which can be achieved by a maximally entangled state, while the maximum value of χ for states consistent with local hidden variable (LHV) models is 2. Thus, any experiment showing a violation of $\chi > 2$ will rule out LHV theories. However, so far, no conclusive experimental violation [63–73] exists due to the difficulties in closing the locality, detection, and postselection loopholes.

It should be emphasized that for the purpose of ruling out LHV theories, any such experiments do not have to assume quantum mechanics to hold, let alone a quantum channel that emits qubit signals. In this case, when a double-click event occurs, one may apply any bit assignment scheme (such as a random bit assignment scheme) to this event without regard to the question of compatibility with any qubit squash model. On the other hand, our universal squash model becomes relevant when the

CHSH violation is used in a quantum context. We may consider the problem of characterizing a multi-photon pair source with respect to a perfectly entangled qubit pair source by checking the measurement statistics of the actual source. This is in the spirit of the idea of self-testing quantum apparatus first proposed by Mayers and Yao [29, 30]. Along a similar line are device-independent QKD based on Bell's inequality [31, 32] and state tomography based on Bell's inequality [33].

To illustrate the applicability of our model to Bell's inequality testing, let us consider quantum state tomography based on Bell's inequality [33]. Bardyn *et al.* [33] have considered the problem of quantifying the closeness of an unknown entangled state emitted by a black box to ideal entangled states by simply testing the unknown state for its CHSH violation. For entanglement sources that emit qubit pairs, they showed that the fidelity F for characterizing the closeness to maximally entangled two-qubit states is bounded by

$$F \geq (1 + \sqrt{[\chi_{\text{obs}}/2]^2 - 1})/2 \quad (30)$$

where χ_{obs} is the observed CHSH violation. Our result allows the application of Eq. (30) even in situations where practical entanglement sources that may emit pairs of multi-photon signals and threshold detectors are used. In the end, we may regard the practical source as a two-qubit entangled source having certain fidelity to a maximally entangled state.

For the CHSH-inequality test, suppose that the number of bits for bases A_i and B_j is $N_{A_i B_j}$, which can be decomposed as $N_{A_i B_j} = N_{A_i B_j}^{s,+} + N_{A_i B_j}^{s,-} + N_{A_i B_j}^d$ where $N_{A_i B_j}^{s,\pm}$ and $N_{A_i B_j}^d$ are the single-click events corresponding to the ± 1 outcome of the measurement $A_i \otimes B_j$ and double-click events, respectively. Then, $E[A_i B_j]$ is bounded by

$$\begin{aligned} E_{ij}^L &= \frac{N_{A_i B_j}^{s,+} - N_{A_i B_j}^{s,-} - N_{A_i B_j}^d}{N_{A_i B_j}} \leq E[A_i B_j] \\ &\leq \frac{N_{A_i B_j}^{s,+} - N_{A_i B_j}^{s,-} + N_{A_i B_j}^d}{N_{A_i B_j}} = E_{ij}^U, \end{aligned} \quad (31)$$

and the CHSH violation χ can be bounded by combining the corresponding bounds for the various $E[A_i B_j]$'s:

$$\begin{aligned} E_{11}^L + E_{12}^L + E_{21}^L - E_{22}^U &\leq \chi \\ &\leq E_{11}^U + E_{12}^U + E_{21}^U - E_{22}^L. \end{aligned} \quad (32)$$

Corollary 2. (CHSH-based source estimation) We regard the original entangled state processed by the squash operation $\Lambda_{n \rightarrow 1}$ on each side of the state in Situation 1 as the *effective two-qubit state*. We bound the CHSH violation of the effective two-qubit state using Eqs. (31)-(32) and infer its fidelity with Eq. (30).

VII. CONCLUSIONS

The use of threshold detectors has been a major obstacle in bridging the practical experiments on quantum protocols and their theoretical qubit-based analyses. In this paper, we provide a universal solution to this for a wide range of protocols including single-qubit-based schemes for QKD, quantum state tomography, and entanglement verification. This allows the translation of existing analyses that assume single-photon inputs to ones that can handle multiple-photon inputs detected with threshold detectors. For future work, it will be interesting to explore the applicability of our universal squash model in other contexts such as quantum metrology [74] and linear optics quantum computation [75].

Acknowledgments — We thank enlightening discussions with Norbert Lütkenhaus and Kiyoshi Tamaki. This work is supported by RGC grants No. HKU 701007P and 700709P of the HKSAR Government, the CRC program, CIFAR, NSERC, and QuantumWorks.

Appendix A: Proof of Theorem 1

1. Statistical Equivalence of Situations 1 and 2 for projective measurements

We show that the bit value outputs of Situations 1 and 2 have the same statistics for any n -photon input state and any unitary transform. This result is non-trivial since it means that the quantum squash operation can be perfectly substituted by a classical operation. We show this by proving that (i) the squash operation commutes with the unitary transform and (ii) directly verifying that the statistics of a single-photon detection after squash is the same as the statistics of a multi-photon detection followed by our classical post-processor.

For (i), it follows from the fact that the original state ρ lives in a tensor product space of n qubits and standard linear optics transformations act on each photon separately. Thus, when the transformation is characterized by a unitary transform U on one qubit, the transformation on the n -qubit state is $\rho' := U^{\otimes n} \rho (U^\dagger)^{\otimes n}$. It can easily be checked that $\Lambda_{n \rightarrow 1}(\rho') = U \Lambda_{n \rightarrow 1}(\rho) U^\dagger$. Here, U^\dagger denotes the adjoint of U .

For (ii), we consider whether the statistics of a single-photon detection after squashing ρ' is the same as the statistics of a PNR detection on ρ' followed by our classical post-processor. We can verify this by comparing the probabilities of producing bits “0” and “1” in the two cases. In some sense this means that squash commutes with the final detection. Due to the bosonic symmetry, the state ρ' is symmetric on exchange of the photons (e.g., $\langle 001 | \rho' | 001 \rangle = \langle 010 | \rho' | 010 \rangle = \langle 100 | \rho' | 100 \rangle$ for a 3-photon state ρ'). In light of this symmetry, we denote the probability of ρ' collapsing to $|\mathbf{x}\rangle$ in a PNR detection as $\lambda_{n-k,k} := \langle \mathbf{x} | \rho' | \mathbf{x} \rangle$ where \mathbf{x} is an n -bit string containing $n-k$ “0”s and k “1”s. For example,

$\langle 001|\rho'|001\rangle = \langle 010|\rho'|010\rangle = \langle 100|\rho'|100\rangle = \lambda_{2,1}$. Normalization gives $\sum_{k=0}^n \binom{n}{k} \lambda_{n-k,k} = 1$.

We now consider the outcome probabilities in Situation 2 where the detectors are PNR and their results are processed by a classical post-processor whose behaviour is defined in Fig. 3. In general, for an n -photon state,

$$p_0^{CP} = \sum_{k=0}^n \binom{n}{k} \frac{n-k}{n} \lambda_{n-k,k} \quad (\text{A1})$$

$$p_1^{CP} = \sum_{k=0}^n \binom{n}{k} \frac{k}{n} \lambda_{n-k,k}. \quad (\text{A2})$$

Next, we consider the outcome probabilities in Situation 1 where a squash is followed by a single-photon detection. The probability of getting 0 is

$$p_0^{SQ} = \langle 0|\Lambda_{n \rightarrow 1}(\rho')|0\rangle. \quad (\text{A3})$$

Expanding the partial trace of the squash operation with the assumption of tracing over qubits 2 to n , we get

$$p_0^{SQ} = \sum_{i_2, \dots, i_n=0,1} \langle 0i_2 \dots i_n|\rho'|0i_2 \dots i_n\rangle \quad (\text{A4})$$

$$= \sum_{k=0}^{n-1} \binom{n-1}{k} \lambda_{n-k,k}. \quad (\text{A5})$$

Similarly, the probability of getting 1 is

$$p_1^{SQ} = \sum_{k=0}^{n-1} \binom{n-1}{k} \lambda_{k,n-k}. \quad (\text{A6})$$

It can be easily checked that $p_0^{CP} = p_0^{SQ}$ and $p_1^{CP} = p_1^{SQ}$ for all n . This means that the squash operation commutes with the final detection. Since (i) works for any arbitrary basis, this proves Theorem 1. Note that here we only focus on projective measurements. However, Theorem 1 also holds for generalized measurements (see Subsection A 2 next).

Had we used PNR detectors in practice (i.e., Situation 2), we would apply Theorem 1 to argue that we had a quantum channel that emits a single qubit to be detected since the squash operation in Situation 1 in connection with the original multi-qubit channel can be regarded as an effective single-qubit channel. This means that it is valid to apply the result of any single-qubit-based analysis. However, when we use threshold detectors instead of PNR detectors, we have to make additional arguments, through Situations 3, 4, and 5, to justify the use of single-qubit-based analyses.

2. Statistical equivalence of Situations 1 and 2 for generalized measurements

We show that Theorem 1 also holds for generalized measurements by extending the proof of the previous Subsection A 1. Suppose that the detection setup in Situations 1 and 2 is a POVM $\{M_i, i = 1, \dots, m\}$ on a

qubit instead of a simple projection onto $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. The i th PNR detector in Situation 2 indicates the number of clicks n_i for the POVM element M_i . Due to the bosonic symmetry of the n -photon state ρ' [76], we denote the probability of collapsing it to (x_1, \dots, x_n) in the PNR detection in Situation 2 as $\lambda_{n_1, \dots, n_m} := \text{Tr}(M_{x_1} \otimes \dots \otimes M_{x_n} \rho')$ where x_1, \dots, x_n each contains a POVM element index $[1, m]$ and there are n_i number of them with index i . For example, $\text{Tr}(M_1 \otimes M_1 \otimes M_2 \otimes M_3 \rho') = \text{Tr}(M_3 \otimes M_1 \otimes M_2 \otimes M_1 \rho') = \lambda_{2,1,1}$ for a 3-element POVM ($m = 3$) and a 4-photon state ($n = 4$). Normalization gives

$$\sum_{\substack{n_1 + \dots + n_m = n \\ n_1, \dots, n_m \geq 0}} \binom{n}{n_1, \dots, n_m} \lambda_{n_1, \dots, n_m} = 1. \quad (\text{A7})$$

We define the classical post-processor in Situation 2 to output outcome $i \in [1, \dots, m]$ with probability n_i/n , when there are n_i photons detected in the i th PNR detector. Thus, the probability of getting outcome i in Situation 2 is

$$p_i^{CP} = \sum_{\substack{n_1 + \dots + n_m = n \\ n_1, \dots, n_m \geq 0}} \binom{n}{n_1, \dots, n_m} \frac{n_i}{n} \lambda_{n_1, \dots, n_m}. \quad (\text{A8})$$

We now turn to the probability of getting outcome i in Situation 1:

$$p_i^{SQ} = \text{Tr}(M_i \Lambda_{n \rightarrow 1}(\rho')). \quad (\text{A9})$$

We arbitrarily choose to trace over photons 2 to n :

$$\begin{aligned} \Lambda_{n \rightarrow 1}(\rho') &= \text{Tr}_{2, \dots, n}(\rho') \\ &= \text{Tr}_{2, \dots, n} \left(\sum_{\substack{x_2, \dots, x_n \\ \in [1, m]}} M_{x_2} \otimes \dots \otimes M_{x_n} \rho' \right). \end{aligned} \quad (\text{A10})$$

Thus, we have

$$\begin{aligned} p_i^{SQ} &= \sum_{\substack{x_2, \dots, x_n \\ \in [1, m]}} \text{Tr}(M_i \otimes M_{x_2} \otimes \dots \otimes M_{x_n} \rho') \\ &= \sum_{\substack{n_1 + \dots + n_m = n-1 \\ n_1, \dots, n_m \geq 0}} \binom{n-1}{n_1, \dots, n_m} \lambda_{n_1, \dots, n_i+1, \dots, n_m} \end{aligned} \quad (\text{A11})$$

which can easily be verified to be equal to Eq. (A8). That is $p_i^{CP} = p_i^{SQ}$ for $i = 1, \dots, m$.

Appendix B: Derivation for the six-state QKD protocol

The constraints for the six-state protocol are

$$e_Z^{\text{key}} = b_1 + b_2, \quad (\text{B1})$$

$$e_X^{\text{key}} = b_2 + b_3, \quad (\text{B2})$$

$$e_Y^{\text{key}} = b_1 + b_3. \quad (\text{B3})$$

We first find b_2 as follows:

$$b_2 = \frac{e_Z^{\text{key}} + e_X^{\text{key}} - e_Y^{\text{key}}}{2} \quad (\text{B4})$$

which, using Eq. (6), implies

$$\frac{\epsilon - 2\delta}{2(1 - \delta)} \leq b_2 \leq \frac{\epsilon + 2\delta}{2(1 - \delta)}. \quad (\text{B5})$$

The entropy term in the key rate expression in Eq. (7) can be broken down into a sum of a bit-error-correction term and a phase-error-correction term:

$$h(b_0, b_1, b_2, b_3) = H(Z) + H(X|Z) \quad (\text{B6})$$

where

$$H(Z) = h_2(e_Z^{\text{key}}) \quad (\text{B7})$$

$$H(X|Z) = (1 - e_Z^{\text{key}})h_2\left(\frac{b_3}{1 - e_Z^{\text{key}}}\right) + e_Z^{\text{key}}h_2\left(\frac{b_2}{e_Z^{\text{key}}}\right) \quad (\text{B8})$$

$$b_0 = 1 - \sum_{i=1}^3 b_i \quad (\text{B9})$$

$$h_2(x) = -x \log x - (1 - x) \log(1 - x). \quad (\text{B10})$$

We can substitute $b_3 = e_X^{\text{key}} - b_2$ in Eq. (B8) and maximize $H(X|Z)$ over b_2 given its range in Eq. (B5) for fixed e_Z^{key} and e_X^{key} . Without the constraint of Eq. (B5) (i.e., the BB84 case), the maximizing value is $b_2 = e_Z^{\text{key}} e_X^{\text{key}}$. For simplicity, we assume that $2\delta \ll \epsilon \ll 1/2$ so that the lower bound of b_2 in Eq. (B5) is greater than the upper bound of $e_Z^{\text{key}} e_X^{\text{key}}$. Since $H(X|Z)$ is a concave function in b_2 , this lower bound of b_2 is the maximizing value when taking into account the constraint of Eq. (B5). Next, we choose the largest possible value for e_X^{key} in order to maximize $H(X|Z)$. Thus, we arrive at Eqs. (8)-(10).

Appendix C: Passive basis selection

We only consider uniform basis detection here. This means that for a B -basis scheme, the initial received light path is split equally into B paths. A passive detection setup consists of orthogonal projections in multiple bases (see Fig. 6). We can regard that there is only one POVM measurement having many elements. In the case of passive BB84, the POVM is $\{\frac{1}{2}|0_z\rangle\langle 0_z|, \frac{1}{2}|1_z\rangle\langle 1_z|, \frac{1}{2}|0_x\rangle\langle 0_x|, \frac{1}{2}|1_x\rangle\langle 1_x|\}$. Due to Appendix A 2, the statistics of Situations 1 and 2 are equivalent even in the passive-basis-selection case. This establishes one link in the overall argument depicted in Fig. 3. The next step is to establish the other link — the relation between the statistics that are actually observed in Situation 3 (or equivalently Situation 4) and the statistics of the ideal Situation 2. Unlike the active-basis-selection

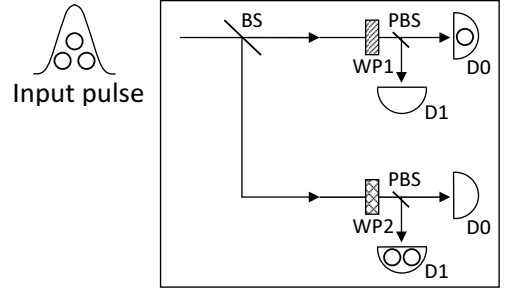


FIG. 6. Detection system used by Bob with passive basis selection among two bases, where a beamsplitter (BS) splits the incoming signal into two paths corresponding to the two bases, two sets of waveplates (WP1 and WP2) each select one of the bases, and a polarizing beamsplitter (PBS) splits the signal into two arms for detection by two threshold detectors (D0 and D1). Here, the incoming signal consists of three photons and one is (two are) collapsed in detector D0 of the first basis (detector D1 of the second basis).

case, the statistics of Situation 2 here have two parts: one for the error rates of the bit values, and one for the statistics of the basis values. Here, we separately consider the two.

We argue that the statistics of basis values in Situation 4 is the same as that of Situation 1 (or equivalently Situation 2), when we adopt a particular basis selection rule for multi-basis events. Thus, once a basis is selected with this rule, it only remains to consider the relation for the bit-value statistics. Fortunately, this second part is the same as that of the active-basis-selection case and we can reuse the previous argument to estimate the error rates with the test bits and discard the double-click key bits.

Now we prove that the basis statistics of Situation 4 with the basis selection rule is the same as the basis statistics of Situation 1. Obviously, in Situation 1, the single photon emitted from the squash operation collapses in each of the B bases with probability $1/B$. In Situation 4, we use the following basis selection rule:

- When only one basis has detection, we choose this basis.
- When $b \leq B$ bases have detection, we choose one among these b bases with uniform probability $1/b$.

The main point is to show that a basis A chosen according to this rule occurs with probability $1/B$, i.e., same as Situation 1. This probability for an n -photon input state is as follows:

$$P(A) := \sum_{b=1}^B \frac{1}{b} \binom{B-1}{b-1} \Pr\{\text{detection in } b \text{ bases including basis } A\} \quad (\text{C1})$$

where

$$P_b := \Pr\{\text{detection in } b \text{ bases including basis } A\}$$

$$= \left(\frac{b}{B}\right)^n - \sum_{c=1}^{b-1} \binom{b}{b-c} P_{b-c} \quad (\text{C2})$$

Here, P_b is defined in terms of a fixed set of b bases of which basis A is an element. The first term in Eq. (C2) represents the probability that each of the n photons collapses in any one basis of this set. Since this term also includes the events that the n photons collapse in less than b bases, we exclude these events in the second term.

Rewriting Eq. (C1) as

$$P(A) = \sum_{b=1}^{B-1} \frac{1}{b} \binom{B-1}{b-1} P_b + \frac{1}{B} P_B \quad (\text{C3})$$

and substituting the expression for P_B from Eq. (C2), we get

$$P(A) = \frac{1}{B}. \quad (\text{C4})$$

This means that by adopting this basis selection rule, the basis statistics of Situation 1 is preserved. The approach to deal with the bit-value statistics is the same as the active-basis-selection case and we can reuse that result to handle the double-click events and to estimate the error rates.

-
- [1] J. S. Bell, *Physics* **1**, 195 (1964).
 - [2] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).
 - [3] C. H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, 1984) pp. 175–179.
 - [4] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002); H.-K. Lo and N. Lütkenhaus, *Physics in Canada* **63**, 191 (2007).
 - [6] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Nature* **464**, 1021 (2010).
 - [7] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, *Phys. Rev. Lett.* **86**, 5807 (2001).
 - [8] D. DiVincenzo, D. Leung, and B. Terhal, *IEEE Trans. Inform. Theory* **48**, 580 (2002).
 - [9] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature* **414**, 413 (2001).
 - [10] J. Bréguet, A. Muller, and N. Gisin, *Journal of Modern Optics* **41**, 2405 (1994).
 - [11] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, *Applied Physics Letters* **70**, 793 (1997).
 - [12] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, *Phys. Rev. Lett.* **96**, 070502 (2006).
 - [13] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Nature* **390**, 575 (1997).
 - [14] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, *Phys. Rev. Lett.* **92**, 047904 (2004).
 - [15] J. F. Sherson, H. Krauter, R. K. Olsson, B. Julsgaard, K. Hammerer, I. Cirac, and E. S. Polzik, *Nature* **443**, 557 (2006).
 - [16] S. Olmschenk, D. N. Matsukevich, P. Maunz, D. Hayes, L.-M. Duan, and C. Monroe, *Science* **323**, 486 (2009).
 - [17] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
 - [18] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, *Phys. Rev. Lett.* **76**, 4656 (1996).
 - [19] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, *Nature Physics* **4**, 282 (2008).
 - [20] H. J. Kimble, *Nature* **453**, 1023 (2008).
 - [21] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, *Phys. Rev. Lett.* **96**, 070504 (2006).
 - [22] M. Paris and J. Řeháček, eds., *Quantum State Estimation, Lecture Notes in Physics*, Vol. 649 (Springer, Heidelberg, 2004).
 - [23] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Quant. Info. Compu.* **5**, 325 (2004).
 - [24] T. Tsurumaru and K. Tamaki, *Phys. Rev. A* **78**, 032302 (2008).
 - [25] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, *Phys. Rev. Lett.* **101**, 093601 (2008).
 - [26] T. Moroder, O. Gühne, N. Beaudry, M. Piani, and N. Lütkenhaus, *Phys. Rev. A* **81**, 052342 (2010).
 - [27] A. A. Semenov and W. Vogel, (2010), e-print arXiv:1004.3700 [quant-ph].
 - [28] The apparent violation is due to the discarding of double-click events and can be fixed by randomly assigning a bit value to them and keeping them.
 - [29] D. Mayers and A. Yao, in *FOCS '98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, USA, 1998) pp. 503–509.
 - [30] D. Mayers and A. Yao, *Quant. Info. Compu.* **4**, 273 (2004).
 - [31] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007).
 - [32] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *New J. Phys.* **11**, 045021 (2009).
 - [33] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, *Phys. Rev. A* **80**, 062327 (2009).
 - [34] D. Mayers, *J. of ACM* **48**, 351 (2001), preliminary version in Mayers, D. *Advances in Cryptology-Proc. Crypto '96*, vol. 1109 of *Lecture Notes in Computer Science*, Koblitz, N. Ed. (Springer, New York, 1996), pp. 343–357.
 - [35] H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
 - [36] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
 - [37] R. Renner and R. König, in *Proc. of the Second Theory of Cryptography Conference (TCC) 2005, Lecture Notes in Computer Science*, Vol. 3378 (Springer, Berlin, 2005) pp. 407–425.

- [38] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
- [39] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
- [40] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
- [41] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
- [42] H. Inamori, N. Lütkenhaus, and D. Mayers, European Physical Journal D **41**, 599 (2007).
- [43] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, IBM Technical Disclosure Bulletin **26**, 4363 (1984).
- [44] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
- [45] We note that there are other ways to tackle the threshold detection problem. In particular, a separating approach was used to justify the use of threshold detectors specifically for the BBM92 protocol [77] and the BB84 protocol [78, 79] without considering squash. Also, Kato and Tamaki [80] proved the security of the six-state protocol with active basis selection and threshold detection by direct calculation of conditional entropy and application of Koashi's security proof based on complementarity scenario [81].
- [46] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005); C.-H. F. Fung and H.-K. Lo, Phys. Rev. A **74**, 042342 (2006).
- [47] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004); K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302(R) (2006).
- [48] M. Koashi, (2005), e-print arXiv:quant-ph/0507154; D. Shirokoff, C.-H. F. Fung, and H.-K. Lo, Phys. Rev. A **75**, 032341 (2007).
- [49] K. Chen and H.-K. Lo, Quant. Info. Compu. **7**, 689 (2007).
- [50] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, (2010), e-print arXiv:1003.1050.
- [51] D. Gottesman and H.-K. Lo, IEEE Trans. Inform. Theory **49**, 457 (2003).
- [52] We note that our formalism and result are fully consistent with the standard Hong-Ou-Mandel effect [82] in quantum optics because we have imposed bosonic symmetry in our wave function.
- [53] One such attack is the following. For each qubit sent by Alice, Eve does nothing to the qubit with probability $1 - p_1 - p_2$ and processes the qubit with probability $p_i/3$, $i = 1, 2$ with the following copying operation in each of the bases $W = X, Y, Z$:

$$\alpha|0_W\rangle + \beta|1_W\rangle \rightarrow \alpha|0_W\rangle_B^{\otimes i}|0_W\rangle_E + \beta|1_W\rangle_B^{\otimes i}|1_W\rangle_E$$
where $i = 1, 2$ output qubits are sent to Bob and one is kept by Eve. Thus, when Eve launches the copying operation in Z with $i = 2$ and Bob detects in the basis X , he gets bit 0, bit 1, and a double click with probabilities $1/4$, $1/4$, and $1/2$, respectively. The asymptotic error probabilities are bounded by

$$2\left(\frac{p_1}{6} + \frac{p_2}{12}\right) \leq e_X, e_Y, e_Z \leq 2\left(\frac{p_1}{6} + \frac{p_2}{12} + \frac{p_2}{6}\right).$$
- [54] H.-K. Lo, Quant. Info. Compu. **1**, 81 (2001).
- [55] The single-photon six-state protocol achieves a tolerable bit error rate of 12.6% with one-way error reconciliation whereas the single-photon BB84 protocol achieves 11.0%.
- [56] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
- [57] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
- [58] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
- [59] A. G. White, D. F. V. James, P. H. Eberhard, and P. G. Kwiat, Phys. Rev. Lett. **83**, 3103 (1999).
- [60] L. K. Shalm, R. B. A. Adamson, and A. M. Steinberg, Nature **457**, 67 (2009).
- [61] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Phys. Rev. A **64**, 052312 (2001).
- [62] G. G. Stokes, Trans. Cambridge Philos. Soc. **9**, 399 (1852).
- [63] S. J. Freedman and J. F. Clauser, Phys. Rev. Lett. **28**, 938 (1972).
- [64] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).
- [65] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
- [66] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998).
- [67] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Nature **409**, 791 (2001).
- [68] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe, Phys. Rev. Lett. **100**, 150404 (2008).
- [69] R. García-Patrón, J. Fiurásek, N. J. Cerf, J. Wenger, R. Tualle-Brouiri, and P. Grangier, Phys. Rev. Lett. **93**, 130409 (2004).
- [70] C. Simon and W. T. M. Irvine, Phys. Rev. Lett. **91**, 110405 (2003).
- [71] P. G. Kwiat, P. H. Eberhard, A. M. Steinberg, and R. Y. Chiao, Phys. Rev. A **49**, 3209 (1994).
- [72] S. Aerts, P. Kwiat, J.-A. Larsson, and M. Żukowski, Phys. Rev. Lett. **83**, 2872 (1999).
- [73] G. Lima, G. Vallone, A. Chiuri, A. Cabello, and P. Mataloni, Phys. Rev. A **81**, 040101 (2010).
- [74] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **96**, 010401 (2006).
- [75] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).
- [76] We consistently use the same notation ρ' here to denote the state after a unitary transformation corresponding to active basis selection.
- [77] M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto, (2008), e-print arXiv:0804.0891 [quant-ph].
- [78] M. Koashi, New J. Phys. **11**, 045018 (2009).
- [79] M. Koashi, (2006), e-print arXiv:quant-ph/0609180.
- [80] G. Kato and K. Tamaki, (2010), e-print arXiv:1008.4663 [quant-ph].
- [81] M. Koashi, (2007), e-print arXiv:0704.3661 [quant-ph].
- [82] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).